

US-PAT-NO: 6560581

DOCUMENT-IDENTIFIER: US 6560581 B1

TITLE: System and method for secure
electronic commerce
transaction

----- KWIC -----

Brief Summary Text - BSTX (9):

This invention provides an electronic commerce system that facilitates commercial interchange of documents and instruments in a large, unrestricted audience of participants, while supporting the underlying principles of authenticity, integrity, privacy, and security. The electronic commerce system has a credential binding server at a trusted credential authority and multiple computing units at associated participants. The credential binding server and

the multiple computing units are interconnected by a communication system, which is publicly available and can be already in existence. Example communication systems include an interactive television system, a credit card network, an ATM (Asynchronous Transfer Mode) switching network, a public network, a wide area network, a satellite network, and an RF network.

Brief Summary Text - BSTX (17):

The electronic commerce system according to this invention can be implemented with existing commercial systems. In one implementation, the commerce system is incorporated into a credit card system to facilitate purchase transactions between a consumer and a merchant, while complementing the existing credit card network that performs the payment card authorization and settlement process between the acquiring and issuing banks. In another implementation, the commerce system is incorporated into an interactive

television system.

Detailed Description Text - DETX (5):

Computing units 24(a), 24(b), and 24(c) are provided at respective ones of the participants 22(a), 22(b), and 22(c). The computing units are depicted for illustration purposes as IBM(.RTM.-compatible personal computers, although other forms of computing units may be used. For instance, the computing units might be embodied as conventional computers (such as mainframe computers, servers, PCs, laptops, notebooks, etc.) or as other computational machines, such as banking ATMs (automated teller machines) and set-top boxes used in an interactive television system.

Detailed Description Text - DETX (7):

The computing units 24(a), 24(b), and 24(c) and computer server 28 are interconnected with each other via one or more communication systems. The communication systems can be embodied as a

wire-based or wireless network.

Examples of communications systems include an ATM (asynchronous transfer mode) switching network, a public network, a wide area network, an interactive television (ITV) network, a credit card network, a satellite network, and an RF network.

Detailed Description Text - DETX (117):

The above discussion presents a general structure of an electronic commerce system. The following two cases provide example implementations of the electronic commerce system in specific commerce environments. The first example implementation is a credit card system and will be described with reference to FIGS. 17 and 18. The second example implementation is an interactive television system and will be described with reference to FIG. 23. In addition to these specific examples, the electronic commerce system can be implemented in a wide variety of commercial environments, including on-line

services and debit or other banking card transactions.

Detailed Description Text - DETX (152):

FIG. 23 diagrammatically illustrates an interactive television (ITV) system 400 that implements the electronic commerce system according to another aspect of this invention. The participants include a subscriber 402, a merchant 404, an acquire 406 and a cable operator 408. The subscriber 402 is equipped with a computing unit in the form of a set-top box (STB) 412. The merchant and acquirer each have a server 414 and 416, respectively, and the cable operator 408 is equipped with a headend server 418. Each computing unit is loaded with an ITV commerce application and a cryptography system to satisfy the security, privacy, integrity, and authenticity aspects of the ITV system. In this implementation, the ITV commerce application can be downloaded from the headend server to the STBs as requested, rather than remaining resident at the STB.

The cryptography system, however, would reside and be executable at the STB.

Detailed Description Text - DETX (153):

The subscriber STB 412 and merchant server 414 are interconnected with the headend server 418 via an interactive network structure, which is represented by the network cloud 420. One example implementation of the network structure is a hybrid fiber-optic/cable distribution system employing digital switching technologies such as asynchronous transfer mode (ATM) for bi-directional communications between the headend and individual subscriber/merchants. This multi-tier distribution system includes a high-speed, high-bandwidth fiber optic cable coupled between the headend and many regional distribution nodes. Each distribution node is then connected to multiple set-top boxes within the region via conventional home entry lines, such as twisted-pair telephone lines or coaxial cable. As an example, a single headend might service 250,000 or

more subscribers, and each regional distribution node might support approximately 1200 subscribers. As technology continues to improve, parts of the ITV network structure can be replaced with wireless forms of communication, such as RF communication or satellite communication.

Detailed Description Text - DETX (159):

Another benefit is that the encrypted and signed packages are independent entities that can be transported by any communication protocol and system. This allows the electronic commerce system to operate over the communication system that already exists between the participants, such as phone networks, on-line services networks, wide area networks, interactive television networks, etc.

Claims Text - CLTX (5):

5. An interactive television system incorporating an electronic system as

recited in claim 4.

Current US Cross Reference Classification -
CCXR (3):
705/26